Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1835 09/02/16

~ "Guccifer" Is Sentenced ~ People Are Talking! ~ KickassTorrents Bust!

~ NX Back to Cartridges? ~ iOS Flaw Affects Mac Too ~ War on Encryption!

~ Bigfoot Family for 2600 ~ VMU Getting Pokemon Go? ~ Linux’s 25th B-day!

-* State Election Systems Hacked *-
-* Call of Duty: Infinite Warfare! *-
-* The NSA Is Hoarding Vulnerabilities! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Can you believe that the Labor Day weekend is already here?? I’m still trying to figure out where our Spring season went; and we’re already into September! The unofficial last weekend of Summer means vacations are just about a memory, schools are about to start up across the country, and not much time left for barbecues to fire up for those burgers and steaks! I’m just not ready for this! And, to make matters worse, a tropical storm/hurricane is making its way up the east coast! At the moment, it looks like we’re going to miss most of these storms, to no surprise to those of us locked into extreme drought conditions!

It’s probably going to be a quiet next couple of weeks as far as news articles are concerned; these long holiday weekends seem to affect the amount of news - at least the kind of material that we’re interested in reading. So, we’ll just keep plugging away and see where everything leads us.

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Call of Duty: Infinite Warfare Multiplayer!
"""""""""""""""""""""""""""""""""" Nintendo NX Console Returning to Cartridges?

Sega Dreamcast VMU Receiving Pokemon GO Port?

And more!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

Call of Duty: Infinite Warfare Multiplayer - Everything You Need to Know

Activision has released the debut trailer for Call of Duty: Infinite Warfare’s multiplayer. The video was shown during Call of Duty XP and shows how the "fluid momentum-based movement system, player focused map design, and deeper levels of combat customization" intersect to create a feel for Call of Duty multiplayer.

"Infinite Warfare Multiplayer introduces an all-new combat rig system, hundreds of weapons, never-before-seen high-tech equipment, and unique prototype weapon crafting to fuse immersive, frenetic action with innovative new gameplay experiences at every turn," Activision explains.

In a second video, developer Infinity Ward goes in-depth in the various classes that are being introduced to Infinite Warfare’s multiplayer. There’s a deep dive into the customisation options which reinforce the play styles with unique weapons and perk abilities through Rigs.

You already order food, hail cabs, and track finances on your smartphone. Now it s time for one app to rule the house, from doors to lights to heating and AC.

Each of the Rigs is outfitted with distinct payloads that "boost player effectiveness and lethality in combat." Rigs allow for players to have three "persistent perks," which are called Traits. Players get to pick one Payload and one Trait to create their own twist on a play style.

The video below highlights three Rigs. The Warfighter "supports the team by getting fast kills, quickly getting to the objective, and always being on the offensive." Its Claw Payload includes a rapid-fire spreadshot firearm that has ricochet bullets. Its Trait makes scores treaks require a higher point value to attain, but they don’t reset when you die.

The Merc Rig is "designed to clear enemies quickly and with authority." Its Bullcharge Payload includes an armored riot shield that lets you rush enemies and penetrate their defenses. The Infusion Trait will regenerate health faster when damage is taken, so you can stay in a firefight for much longer.

Finally, the FTL Rig is all about being an assassin. It is outfitted with experimental tech and represents "the evolution in covert guerrilla ops." Its Eraser Payload completely vaporises enemies with a compact incinerating handgun. The Powerslide Trait enhances the speed and distance of the slide.

During the event, Activision also announced a multiplayer beta for Call of Duty: Infinite Warfare and it will begin on October 14. The beta will be available on PlayStation 4 on that day. A start date for other platforms hasn’t been announced.

Also during the Call of Duty XP opening briefing, Activision announced that all 16 maps from Call of Duty 4: Modern Warfare will come to Modern Warfare Remastered, eventually.

Nintendo NX Console Is Again Rumored To Return to Cartridges

Nintendo’s next game console may return to using cartridges to sell its titles, according to a Friday report by The Wall Street Journal.

The Nintendo Wii U uses discs for its games, but the company’s next console is reportedly going to move back to the cartridge format.

Citing "people familiar with the matter," the outlet says the company is considering the move back to the older format, which could help keep the device small for portability.

This isn’t the first time we have heard of this possibility. A report by Eurogamer in July said the system would not only use cartridges, but also be playable while both connected to a television as well as on the go.

The report comes a day after the video game maker held its latest Nintendo Direct, during which it announced upcoming 3DS versions of Super Mario Maker and Yoshi’s Woolly World. The company made no announcements regarding the NX, and analysts have told the Journal that an announcement could come before the Tokyo Game Show starts on September 15.

Sega Dreamcast Visual Memory Unit Receiving Pokemon GO Port

Okay, who amongst you reading this remembers the Sega Dreamcast Visual Memory Unit (VMU)? For those that do not remember, it was a removable memory card for the Sega Dreamcast console which doubled as a small gaming on the go device. Since the VMU had a screen, controls and a couple of action buttons, it was easy to see how some developers put games on it. For the most part the Visual Memory Unit was used as a secondary screen while plugged into the controller. Some sports games allowed picking plays on it, Resident Evil put the heart rate monitor on it, etc. Anyhow, Pokemon GO is getting ported to the Sega Dreamcast Visual Memory Unit. Who wants to place a bet on how long before Nintendo and Niantic take it down?

Yep, this is not an official port as if there were any that were reading this thinking it was. The name is sort of misleading as this is not Pokemon GO as in the go outside and play game. This is rather Pokemon GO as in you can play it on the go, like the hand held versions over the years. Either way, the developer is calling it Pokemon GO so I am going with it, just wanted to make sure you all knew what was going on here.

This Sega Dreamcast Visual Memory Unit version of Pokemon GO will feature randomly generated maps and a plethora of Pokemon to catch. Now, considering the limitations of the VMU it is probably not going to include all of the Pokemon and their evolved states. That is just a limitation of the hardware,

folks.

Now, how many believe this is going to get shut down prior to it being released, or right after? I have a hunch it won t be long before Nintendo and/or Niantic drop a Cease and Desist on this one so grab it when it releases in 2017.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
""""""""""""""""""""

Atari 2600 Game Bigfoot Family Currently on Kickstarter

The Atari 2600 and Kickstarter are not exactly synonymous. Most people that want new Atari 2600 games probably already know about AtariAge and their store. If not, they do now. That has not stopped Bobby Alexander from hitting the popular crowdsourcing service to seek assistance in getting his new game on cartridge. Bigfoot Family is a new Atari 2600 game and interesting because it pulls from a classic title to be original.

Before I get underway here I do want to mention that Bigfoot Family was developed by Gemintronic. Jason S. the owner of Gemintronic is a member of our staff here at Retro Gaming Magazine in the capacity of writer. I am covering Bigfoot Family so there is no concern over favoritism. Okay, now that that is out of the way.

Bigfoot Family pulls from Rogue to have completely random levels. For those that do not know, Rogue is a classic game that was initially created using ASCII graphics- letters and numbers on your keyboard- to create the worlds. While the Atari 2600 is not exactly a powerhouse in the ASCII graphics world, Bigfoot Family does make use of colored blocks to create the game world you traverse.

The story of Bigfoot Family is one that most fathers and husbands can relate to. Bigfoot wakes up and realizes his wife and child are missing. He leaves his cave thinking they are outside gathering food or playing- nowhere to be found. This sets Bigfoot off in a rage of concern, as it would any parent and husband. There is a time limit and there are more than one enemy to be wary of in Bigfoot Family.

Bigfoot Family is currently on Kickstarter looking for a modest $800 goal. There is just under 30 days left in the funding effort. If you want to support independently developed and published games then check this one out. The price for a cart is quite reasonable. There is also a complete package which includes a poster, stickers, manual, box and cart (of course).

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

FBI Says Foreign Hackers Penetrated State Election Systems

The FBI has uncovered evidence that foreign hackers penetrated two state election databases in recent weeks, prompting the bureau to warn election officials across the country to take new steps to enhance the security of their computer systems, according to federal and state law enforcement officials.

The FBI warning, contained in a flash alert from the FBI s Cyber Division, a copy of which was obtained by Yahoo News, comes amid heightened concerns among U.S. intelligence officials about the possibility of cyberintrusions, potentially by Russian state-sponsored hackers, aimed at disrupting the November elections.

Those concerns prompted Homeland Security Secretary Jeh Johnson to convene a conference call with state election officials on Aug. 15, in which he offered his department s help to make state voting systems more secure, including providing federal cybersecurity experts to scan for vulnerabilities, according to a readout of the call released by the department.

Johnson emphasized in the call that Homeland Security was not aware of specific or credible cybersecurity threats to the election, officials said. But three days after that call, the FBI Cyber Division issued a potentially more disturbing warning, titled Targeting Activity Against State Board of Election Systems. The alert, labeled as restricted for NEED TO KNOW recipients, disclosed that the bureau was investigating cyberintrusions against two state election websites this summer, including one that resulted in the exfiltration, or theft, of voter registration data. It was an eye opener, a senior law enforcement official said of the bureau s discovery of the intrusions. We believe it s kind of serious, and we re investigating.

The bulletin does not identify the states in question, but sources familiar with the document say it refers to the targeting by suspected foreign hackers of voter registration databases in Arizona and Illinois. In the Illinois case, officials were forced to shut down the state s voter registration system for 10 days in late July, after the hackers managed to download personal data on up to 200,000 state voters, Ken Menzel, the general counsel of the Illinois Board of Elections, said in an interview. The Arizona attack was more limited, involving malicious software that was introduced into its voter registration system but no successful exfiltration of data, a state official said.

The FBI bulletin listed eight separate IP addresses that were the sources of the two attacks and suggested that the attacks may have been linked, noting that one of the IP addresses was used in both intrusions. The bulletin implied that the bureau was looking for any signs that the attacks may have attempted to target even more than the two states. The FBI is requesting that states contact their Board of Elections and determine if any similar activity to their logs, both inbound and outbound, has been detected, the alert reads. Attempts should not be made to touch or ping the IP addresses directly.

This is a big deal, said Rich Barger, chief intelligence officer for ThreatConnect, a cybersecurity firm, who reviewed the FBI alert at the request of Yahoo News. Two state election boards have been popped, and data has been taken. This certainly should be concerning to the common American voter.

Barger noted that one of the IP addresses listed in the FBI alert has surfaced before in Russian criminal underground hacker forums. He also said the method of attack on one of the state election systems including the types of tools used by the hackers to scan for vulnerabilities and exploit them appears to resemble methods used in other suspected Russian state-sponsored cyberattacks, including one just this month on the World Anti-Doping Agency.

The FBI did not respond to detailed questions about the alert, saying in a statement only that such bulletins are provided to help systems administrators guard against the actions of persistent cyber criminals. Menzel, the Illinois election official, said that in a recent briefing, FBI agents confirmed to him that the perpetrators were believed to be foreign hackers, although they were not identified by country. He said he was told that the bureau was looking at a possible link to the recent highly publicized attack on the Democratic National Committee and other political organizations, which U.S. officials suspect was perpetrated by Russian government hackers. But he said agents told him they had reached no conclusions, and other experts say the hackers could also have been common cybercriminals hoping to steal personal data on state voters for fraudulent purposes, such as obtaining bogus tax refunds.

Still, the FBI warning seems likely to ramp up pressure on the Department of Homeland Security to formally designate state election systems as part of the nation s critical infrastructure requiring federal protection a key step, advocates say, in forestalling the possibility of foreign government meddling in the election.

Such a formal designation, which would allow state election officials to request federal assistance to protect their voting systems, is under consideration, a Homeland Security spokesman told Yahoo News.

Federal and state election officials say that the prospect of a full-blown cyberattack that seriously disrupts the November elections is remote, but not out of the question. About 40 states use optical-scan electronic-voting machines, allowing voters to fill out their choices on paper. The results are tabulated by computers.

These are reasonably safe because the voting machines are backed up by paper ballots that can be checked, says Andrew W. Appel, a Princeton University computer science professor who has studied election security. But six states and parts of four others (including large swaths of Pennsylvania, a crucial swing state in this year s race) are more vulnerable because they rely on paperless touchscreen voting, known as DREs or Direct-Recording Electronic voting machines, for which there are no paper ballot backups.

Then whatever numbers the voting computer says at the close of the polls are completely under the control of the computer program in there, Appel wrote in a recent blog post titled Security Against Election Hacking. If the computer is hacked, then the hacker gets to decide what numbers are reported. All DRE (paperless touchscreen) voting computers are susceptible to this kind of hacking. This is our biggest problem. Another area of concern cited by Appel and other experts is the growing number of states that allow overseas and military voters to cast their ballots online.

In his conference call this month with state election officials, Johnson urged them to guard against potential intrusions by taking basic precautionary steps, such as ensuring that electronic voting machines are not connected to the Internet while voting is taking place. The FBI bulletin addresses additional potential threats, such as the targeting of state voter registration databases comparable to the attacks in Arizona and Illinois. This is a wake-up call for other states to look at their systems, said Tom Hicks, chairman of the federal Election Assistance Commission, an agency created by Congress after the 2000 Florida recount to protect the integrity of elections and which helped distribute the FBI alert to state election officials last week.

Hackers could conceivably use intrusions into voter registration databases to delete names from voter registration lists, although in most states, voters can request provisional ballots at the polls, allowing time for discrepancies to be resolved, an official of the National Association of Secretaries of State told Yahoo News. Still, according to Barger, the cybersecurity expert, such attacks can be used to create havoc and sow doubt over the election results.

As a result, the FBI alert urges state officials to take additional steps to secure their systems, including conducting vulnerability scans of their databases. In addition, the bulletin urges officials to sharply restrict access to their databases. Implement the principle of least privilege for database accounts, the FBI alert reads. It adds that any given user should have access to only the bare minimum set of resources required to perform business tasks.

Romanian Hacker ’Guccifer’ Sentenced to 52 Months in U.S. Prison

A Romanian hacker nicknamed "Guccifer" who helped expose the existence of a private email domain Hillary Clinton used when

she was U.S. secretary of state was sentenced on Thursday to 52 months in prison by a federal court in Alexandria, Virginia.

Marcel Lazar, 44, who used the alias online, had pleaded guilty in May to charges including unauthorized access to a protected computer and aggravated identity theft after being extradited from Romania.

Lazar's public defender, Shannon Quill, was not immediately available for comment.

Lazar has said in interviews he breached Clinton's private server at her home in Chappaqua, New York, but law enforcement and national security officials say that claim is meritless.

Lazar is believed to have hacked into email accounts of about 100 victims between 2012 and 2014.

They include prominent political figures such as former Secretary of State Colin Powell, a relative of former President George W. Bush and Sidney Blumenthal, a former Clinton White House aide and an unofficial adviser to Clinton. Clinton is now the Democratic nominee for president.

Lazar leaked online memos Blumenthal sent Clinton that were addressed to her private email account, which was used during her time as secretary of state to conduct both personal and work business in lieu of a government account.

Clinton's email arrangement, which became the subject of an FBI investigation, has drawn intense scrutiny from Republicans attempting to sow doubt about her honesty ahead of the Nov. 8 presidential election.

An entity calling itself "Guccifer 2.0" and claiming to be a Romanian hacker emerged in June and began taking credit for data breaches at the Democratic National Committee and Democratic Congressional Campaign Committee.

U.S. intelligence officials and cyber security experts believe Guccifer 2.0 is a front for Russian intelligence services intended to spread confusion about the hacks against the Democratic Party.

US Unveils Charges Against KickassTorrents, Names Two More Defendants

A total of three men are said to be operators of file-sharing site KickassTorrents (KAT), according to U.S. prosecutors. Last month, federal authorities arrested the 30-year-old Ukrainian mastermind of KAT, Artem Vaulin, and formally charged him with one count of conspiracy to commit criminal copyright infringement, one count of conspiracy to commit money laundering, and two counts of criminal copyright infringement. Two other Ukrainians were named in the new indictment: Levgen (Eugene) Kutsenko and Oleksander (Alex) Radostin. While only Vaulin has been arrested, bench warrants have been issue for

the arrest of all three men. Ars Technica reports:

"Prosecutors say the three men developed and maintained the site together and used it to ’generate millions of dollars from the unlawful distribution of copyright-protected media, including movies, [...] television shows, music, video games, computer software, and electronic books.’ They gave out ’Reputation’ and ’User Achievement’ awards to users who uploaded the most popular files, including a special award for users who had uploaded more than 1,000 torrents. The indictment presents a selection of the evidence that the government intends to use to convict the men, and it isn’t just simple downloads of the copyrighted movies. The government combed through Vaulin’s e-mails and traced the bitcoins that were given to him via a ’donation’ button."

Germany and France Declare War on Encryption To Fight Terrorism

France and Germany are asking the European Union for new laws that would require mobile messaging services to decrypt secure communications on demand and make them available to law enforcement agencies.

French and German interior ministers this week said their governments should be able to access content on encrypted services in order to fight terrorism, the Wall Street Journal reported.

French interior minister Bernard Cazeneuve went on to say that the encrypted messaging apps like Telegram and WhatsApp "constitute a challenge during investigations," making it difficult for law enforcement to conduct surveillance on suspected terrorists.

The proposal calls on the European Commission to draft a law that would "impose obligations on operators who show themselves to be non-cooperative, in particular when it comes to withdrawing illegal content or decrypting messages as part of an investigation."

The proposed laws would force major technology companies including Apple, WhatsApp, Facebook, Telegram, and many others, to build encryption backdoors into their messaging apps.

The European Union has always been a strong supporter of privacy and encryption, but the recent series of terrorist attacks across both France and Germany this summer, including Normandy church attack carried out by two jihadists who reportedly met on Telegram, which made the countries shout for encryption backdoors loudly.

Although the proposal acknowledges encryption to be a critical part in securing communications and financial transactions, it says that solutions must be found to "enable effective investigation" while protecting users privacy.

Privacy advocates have been alarmed by the new proposals, as

recent NSA hack just recently proved all of us that no system is hack-proof for hackers with right hacking skills and sufficient resources.

So, what happened to the NSA, which is the highly sophisticated intelligence agency of the world, could happen to encrypted messaging services that would feature an encryption backdoor for law enforcement.

The European Commission is believed to come up with new laws on privacy and security for telecom operators this fall, which would include third-party services such as WhatsApp or Telegram.

The NSA Is Hoarding Vulnerabilities

The National Security Agency is lying to us. We know that because of data stolen from an NSA server was dumped on the Internet. The agency is hoarding information about security vulnerabilities in the products you use, because it wants to use it to hack others' computers. Those vulnerabilities aren't being reported, and aren't getting fixed, making your computers and networks unsafe.

On August 13, a group calling itself the Shadow Brokers released 300 megabytes of NSA cyberweapon code on the Internet. Near as we experts can tell, the NSA network itself wasn't hacked; what probably happened was that a "staging server" for NSA cyberweapons - that is, a server the NSA was making use of to mask its surveillance activities - was hacked in 2013.

The NSA inadvertently resecured itself in what was coincidentally the early weeks of the Snowden document release. The people behind the link used casual hacker lingo, and made a weird, implausible proposal involving holding a bitcoin auction for the rest of the data: "!!! Attention government sponsors of cyber warfare and those who profit from it !!!! How much you pay for enemies cyber weapons?"

Still, most people believe the hack was the work of the Russian government and the data release some sort of political message. Perhaps it was a warning that if the US government exposes the Russians as being behind the hack of the Democratic National Committee - or other high-profile data breaches - the Russians will expose NSA exploits in turn.

But what I want to talk about is the data. The sophisticated cyberweapons in the data dump include vulnerabilities and "exploit code" that can be deployed against common Internet security systems. Products targeted include those made by Cisco, Fortinet, TOPSEC, Watchguard, and Juniper - systems that are used by both private and government organizations around the world. Some of these vulnerabilities have been independently discovered and fixed since 2013, and some had remained unknown until now.

All of them are examples of the NSA - despite what it and other representatives of the US government say - prioritizing its

ability to conduct surveillance over our security. Here’s one example. Security researcher Mustafa al-Bassam found an attack tool codenamed BENIGHCERTAIN that tricks certain Cisco firewalls into exposing some of their memory, including their authentication passwords. Those passwords can then be used to decrypt virtual private network, or VPN, traffic, completely bypassing the firewalls’ security. Cisco hasn’t sold these firewalls since 2009, but they’re still in use today.

Vulnerabilities like that one could have, and should have, been fixed years ago. And they would have been, if the NSA had made good on its word to alert American companies and organizations when it had identified security holes.

Over the past few years, different parts of the US government have repeatedly assured us that the NSA does not hoard "zero days" › the term used by security experts for vulnerabilities unknown to software vendors. After we learned from the Snowden documents that the NSA purchases zero-day vulnerabilities from cyberweapons arms manufacturers, the Obama administration announced, in early 2014, that the NSA must disclose flaws in common software so they can be patched (unless there is "a clear national security or law enforcement" use).

Later that year, National Security Council cybersecurity coordinator and special adviser to the president on cybersecurity issues Michael Daniel insisted that US doesn’t stockpile zero-days (except for the same narrow exemption). An official statement from the White House in 2014 said the same thing.

Hoarding zero-day vulnerabilities is a bad idea. It means that we’re all less secure. When Edward Snowden exposed many of the NSA’s surveillance programs, there was considerable discussion about what the agency does with vulnerabilities in common software products that it finds. Inside the US government, the system of figuring out what to do with individual vulnerabilities is called the Vulnerabilities Equities Process (VEP). It’s an inter-agency process, and it’s complicated.

There is a fundamental tension between attack and defense. The NSA can keep the vulnerability secret and use it to attack other networks. In such a case, we are all at risk of someone else finding and using the same vulnerability. Alternatively, the NSA can disclose the vulnerability to the product vendor and see it gets fixed. In this case, we are all secure against whoever might be using the vulnerability, but the NSA can’t use it to attack other systems.

There are probably some overly pedantic word games going on. Last year, the NSA said that it discloses 91 percent of the vulnerabilities it finds. Leaving aside the question of whether that remaining 9 percent represents 1, 10, or 1,000 vulnerabilities, there’s the bigger question of what qualifies in the NSA’s eyes as a "vulnerability."

Not all vulnerabilities can be turned into exploit code. The NSA loses no attack capabilities by disclosing the vulnerabilities it can’t use, and doing so gets its numbers up; it’s good PR. The vulnerabilities we care about are the ones in the Shadow Brokers

data dump. We care about them because those are the ones whose existence leaves us all vulnerable.

Because everyone uses the same software, hardware, and networking protocols, there is no way to simultaneously secure our systems while attacking their systems › whoever "they" are. Either everyone is more secure, or everyone is more vulnerable.

Pretty much uniformly, security experts believe we ought to disclose and fix vulnerabilities. And the NSA continues to say things that appear to reflect that view, too. Recently, the NSA told everyone that it doesn't rely on zero days - very much, anyway.

Earlier this year at a security conference, Rob Joyce, the head of the NSA's Tailored Access Operations (TAO) organization - basically the country's chief hacker - gave a rare public talk, in which he said that credential stealing is a more fruitful method of attack than are zero days: "A lot of people think that nation states are running their operations on zero days, but it's not that common. For big corporate networks, persistence and focus will get you in without a zero day; there are so many more vectors that are easier, less risky, and more productive."

The distinction he's referring to is the one between exploiting a technical hole in software and waiting for a human being to, say, get sloppy with a password.

A phrase you often hear in any discussion of the Vulnerabilities Equities Process is NOBUS, which stands for "nobody but us." Basically, when the NSA finds a vulnerability, it tries to figure out if it is unique in its ability to find it, or whether someone else could find it, too. If it believes no one else will find the problem, it may decline to make it public. It's an evaluation prone to both hubris and optimism, and many security experts have cast doubt on the very notion that there is some unique American ability to conduct vulnerability research.

The vulnerabilities in the Shadow Brokers data dump are definitely not NOBUS-level. They are run-of-the-mill vulnerabilities that anyone - another government, cybercriminals, amateur hackers - could discover, as evidenced by the fact that many of them were discovered between 2013, when the data was stolen, and this summer, when it was published. They are vulnerabilities in common systems used by people and companies all over the world.

So what are all these vulnerabilities doing in a secret stash of NSA code that was stolen in 2013? Assuming the Russians were the ones who did the stealing, how many US companies did they hack with these vulnerabilities? This is what the Vulnerabilities Equities Process is designed to prevent, and it has clearly failed.

If there are any vulnerabilities that - according to the standards established by the White House and the NSA - should have been disclosed and fixed, it's these. That they have not been during the three-plus years that the NSA knew about and exploited them - despite Joyce's insistence that they're not

very important - demonstrates that the Vulnerable Equities Process is badly broken.

We need to fix this. This is exactly the sort of thing a congressional investigation is for. This whole process needs a lot more transparency, oversight, and accountability. It needs guiding principles that prioritize security over surveillance. A good place to start are the recommendations by Ari Schwartz and Rob Knake in their report: these include a clearly defined and more public process, more oversight by Congress and other independent bodies, and a strong bias toward fixing vulnerabilities instead of exploiting them.

And as long as I'm dreaming, we really need to separate our nation's intelligence-gathering mission from our computer security mission: we should break up the NSA. The agency's mission should be limited to nation state espionage. Individual investigation should be part of the FBI, cyberwar capabilities should be within US Cyber Command, and critical infrastructure defense should be part of DHS's mission.

I doubt we're going to see any congressional investigations this year, but we're going to have to figure this out eventually. In my 2014 book Data and Goliath, I write that "no matter what cybercriminals do, no matter what other countries do, we in the US need to err on the side of security by fixing almost all the vulnerabilities we find..." Our nation's cybersecurity is just too important to let the NSA sacrifice it in order to gain a fleeting advantage over a foreign adversary.

That Really Scary iOS Security Flaw Also Affects Your Mac

It s time to update.

The same security flaw that could have allowed hackers to steal your iPhone data without you knowing it also exists on the Mac.

On Thursday, Apple released a patch for a security flaw that would allow hackers to exploit flaws in its OS X desktop operating system, install spyware on the computer, and steal all kinds of data. The flaws Apple AAPL 0.94% patches are the same it fixed in iOS 9.3.5 last week.

In a security note, Apple was loath to say much, stipulating as it does with all security updates that it doesn t disclose, discuss, or confirm security issues until an investigation has occurred and patches or releases are available.

However, the tech giant released patches to its desktop operating system that would have allowed hackers to find out where the kernel memory is stored in OS X Yosemite and OS X El Capitan, enabling them to run spyware with full administrator privileges.

In other words, anyone running a Mac should update their computers immediately.

The flaw was originally discovered last month after a human

rights activist in the United Arab Emirates was targeted with a text message containing a link. Had Ahmed Mansoor, the activist, clicked the link, he could have given his hackers access to his operating system and allowed them to steal everything from phone call information to data he stored on his device. What s worse, the spyware lives on undetected by the user and can uninstall itself once the hacker has obtained all the information he or she wants to collect.

Instead of clicking on the link, Mansoor sent the link to watchdog group Citizen Lab, which worked with security firm Lookout to identify the vulnerability. They reported that the tool the hackers were using is called Pegasus and was developed by a company that specializes in cyber weapons and sells those to governments for use against high-value targets.

After the two organizations identified the flaw and how it targeted both the iOS kernel and Apple s own Safari browser, they informed the iPhone maker. Apple patched iOS 10 days later and those running iOS 9.3.5 are now believed to be safe from the hack.

However, it wasn t clear whether the issue also affected Apple s desktop operating system (which will soon be renamed to macOS) until Thursday, when Apple released the same patch and credited both Citizen Lab and Lookout for finding the flaw. Like the iOS version, which is believed to have been targeting devices for several years, the Mac version of the spyware is fully capable of stealing all user data.

Linus on Linux’s 25th Birthday

The creator of Linux, Linus Torvalds, posted his famous message announcing Linux on August 25, 1991, claiming that it was "just a hobby, won’t be big and professional like gnu." ZDNet’s Steven J. Vaughan-Nichols caught up with Linus Torvalds and talked about Linux’s origins in a series of interviews:
"SJVN: What’s Linux real birthday? You’re the proud papa, when do you think it was? When you sent out the newsgroup post to the Minix newsgroup on August 25, 1991? When you sent out the 0.01 release to a few friends?

LT: I think both of them are valid birthdays. The first newsgroup post is more public (August 25), and you can find it with headers giving date and time and everything. In contrast, I don’t think the 0.01 release was ever announced in any public setting (only in private to a few people who had shown interest, and I don’t think any of those emails survived). These days the way to find the 0.01 date (September 17) is to go and look at the dates of the files in the tar-file that still remains. So, both of them work for me. Or either. And, by the way, some people will argue for yet other days. For example, the earliest public semi-mention of Linux was July 3: that was the first time I asked for some POSIX docs publicly on the minix newsgroup and mentioned I was working on a project (but didn’t name it). And at the other end, October 5 was the first time I actually publicly announced a Linux version: ’version 0.02 (+1 (very small) patch already).’ So you might have to buy four cakes if you want to cover all the

eventualities."

Vaughan-Nichols goes on to pick Linus' brain about what he was doing when he created Linux. In honor of Linux's 25th birthday today, let's all sing happy birthday... 1... 2... 3...

=~=~=~=